# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

Please Enter 07/15/04



## REMARKS

Claims 25, 26, 28, 33, 73, 77, 79, 83, 84 and 95-98 are pending. Claims 1-24, 27, 29-32, 34-72, 74-76, 78, 80-82 and 85-94 have been canceled. Claims 25, 28, 33, 73, 79 and 83 are amended herein.

Claims 1-24 (canceled)

25. (currently amended) A copyright protection protocol for protecting copyright of digital contents, said protocol including a header and the digital contents, said digital contents being encrypted, said header including key data for decrypting the digital contents, said key data being randomly generated in response to identity characters of a user transmitted to a host server from a terminal unit, wherein said terminal unit receives said protocol from said host server and replays said digital contents by decrypting the encrypted digital contents in response to the key data, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field;

wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a field for indicating the code of a digital content provider, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating the number of users sharing a personal computer, a field for indicating the number of users sharing a replaying device, a field for indicating user authorization information at the personal computer, and a field for indicating user authorization information at the replaying device; and

wherein the field for indicating user authorization information at the personal computer and

the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of a user key, and a field for indicating the size of the hash value generated by a hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

2. (original) The protocol of claim ~~26~~ 1, further comprising a field for indicating the size of the encrypted digital contents, and an additional information field.

27. (canceled)

3. ~~28.~~ (currently amended) A copyright protection protocol for protecting copyright of digital contents, said protocol including a header and the digital contents, said digital contents being encrypted, said header including key data for decrypting the digital contents, said key data being randomly generated in response to identity characters of a user transmitted to a host server from a terminal unit, wherein said terminal unit receives said protocol from said host server and replays said digital contents by decrypting the encrypted digital contents in response to the key data ~~The protocol of claim 25~~, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, a field for indicating the size of the unencrypted header field, an encrypted header field, and a field for indicating the size of the encrypted header field;

wherein the unencrypted header field comprises a copyright library version field, a digital

content conversion format field, a field for indicating the code of a digital content provider, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating the number of users sharing a personal computer, a field for indicating the number of users sharing a replaying device, a field for indicating user authorization information at the personal computer, and a field for indicating user authorization information at the replaying device; and

wherein the field for indicating user authorization information at the personal computer and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of a user key, and a field for indicating the size of the hash value generated by a hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

Claims 29-32 (canceled)

4. 3

~~33~~. (currently amended) The protocol format of claim ~~27 or 28~~, wherein the encrypted header field comprises a field for an encryption algorithm of the digital content, a field for indicating a basic process unit of the digital content, a field for indicating the number of encrypted bytes, and a hash value field for a hash value for determining a state of the entire header.

Claims 34-72 (canceled)

5.

~~73~~. (currently amended) Apparatus for decrypting and encrypting a digital content,

comprising:

a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user to a service server, receiving and storing key information output from said service server, receiving a protocol including encrypted digital content output from said service server, and decrypting said protocol by using said decryption algorithm and said stored key information; and

said service server, said service server having an encryption algorithm, said service server producing said key information in response to said identity characters transmitted from said terminal unit, transmitting said key information in a header to said terminal unit, encrypting said digital content by using said key information and said encryption algorithm, and transmitting the encrypted digital content along with said header, as said protocol, to said terminal unit ~~The apparatus of claim 70~~, wherein said service server further comprises

a key generation algorithm responsive to said key information for generating a user key, the user key being used for encrypting a temporary validation key generated in response to a user's request, the temporary validation key being used for encrypting said digital content, the user key and the encrypted temporary validation key being used to generate user authorization key information, the header being generated in response to the user authorization key information, wherein said service server further comprises:

an interface for receiving said identity characters transmitted from said terminal unit;

a key information generator for producing said key information in response to said identity characters received by said interface;

a user key generator responding to said key information for generating said user key;

a temporary validation key generator for generating said temporary validation key in response to a user digital content request signal that is input through the interface;

a user authorization information generator responding to said user key for encrypting said temporary validation key to generate user authorization information;

a header generator responding to said user key for generating a header, wherein said header includes said user authorization information; and

a protocol format generator for adding said encrypted digital content to said header to generate said protocol.

74-76. (canceled)

~~77~~ 6. (previously presented) The apparatus of claim ~~73~~ 5, wherein said service server further comprises a database storing a set of identity characters used by said key information generator for comparison with the user's identity characters in order to determine whether the user is a registered user.

78. (canceled)

~~79~~ 7. (currently amended) An apparatus for encrypting and decrypting a digital content, comprising:

a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user to a service server, receiving and storing a key information output from said

service server, receiving a protocol including encrypted digital content output from said service server, and decrypting the encrypted digital content included with said protocol by using said decryption algorithm and said key information;

said service server having an encryption algorithm, said service server transmitting said key information to said terminal unit and transmitting said identity characters to a host server, encrypting said digital content by using said key information and said encryption algorithm, and transmitting said protocol to said terminal unit; and

said host server responding to said identity characters transmitted from said service server for producing said key information, for transmitting said key information to said service server, and for storing a set of user identity characters for comparison to the identity characters transmitted to said host server from said service server, wherein said terminal unit further comprises:

a key generation algorithm responsive to said stored key information for generating a user key, the user key being used for generating and confirming user authorization information by decrypting a temporary validation key in a user authorization information field of the header, said temporary validation key being used for decrypting said encrypted digital content;

an interface for receiving said key information transmitted from said service server;

a user authority identifier utilizing said key information for obtaining the user key after reading the header of the protocol received from the service server and identifying whether said user is authorized to receive said digital content by analyzing the user authorization information with the user key;

a temporary validation key decryptor for decrypting said temporary validation key by

using the user key provided by said user authorization identifier; and

a digital content decryptor for decrypting said encrypted digital content by using the temporary validation key decrypted by the temporary validation key decryptor.

Claims 80-82 (canceled)

83. (currently amended) An apparatus for encrypting and decrypting a digital content, comprising:

a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user to a service server, receiving and storing a key information output from said service server, receiving a protocol including encrypted digital content output from said service server, and decrypting the encrypted digital content included with said protocol by using said decryption algorithm and said key information;

said service server having an encryption algorithm, said service server transmitting said key information to said terminal unit and transmitting said identity characters to a host server, encrypting said digital content by using said key information and said encryption algorithm, and transmitting said protocol to said terminal unit; and

said host server responding to said identity characters transmitted from said service server for producing said key information, for transmitting said key information to said service server, and for storing a set of user identity characters for comparison to the identity characters transmitted to said host server from said service server, wherein said service server comprises:

a key generation algorithm responsive to said key information for generating a user key, the

user key being used for encrypting a temporary validation key generated in response to a user's request, the temporary validation key being used for encrypting said digital content, the user key and the encrypted temporary validation key being used to generate user authorization key information, the header being generated in response to the user authorization key information ~~The apparatus of claim 82~~, wherein said service server further comprises:

an interface for receiving said identity characters transmitted from said terminal unit and transmitting said identity characters to said host server;

a user key generator responding to said key information for generating said user key;

a temporary validation key generator, responding to said user's request, for generating said temporary validation key;

a user authorization information generator responding to said user key for encrypting said temporary validation key to generate said user authorization information;

a header generator responding to said encrypted temporary validation key for generating the header, wherein said header includes said user authorization information; and

a protocol format generator for adding said encrypted digital content to said header to generate said protocol.

9. ~~84~~. (previously presented) The apparatus of claim ~~83~~ 8, wherein said host server comprises:

a key information generator and a database, said database storing said set of user identity characters and corresponding key information, said key information generator checking said data base for user identity characters corresponding to the identity characters transmitted from said interface, said key information generating new key information when it is determined that said

database does not include a set of user identity characters corresponding to said identity characters transmitted from said interface and providing the new key information to said user key generator, and when said database does include a set of user identity characters corresponding to said identity characters transmitted from said interface and providing, providing the stored corresponding key information to said user key generator.

Claims 85-94 (canceled)

10.

95. (previously presented) A method of digital content encryption and decryption in a digital content transmission system, the method comprising steps of:

generating key information using random numbers, said key information corresponding to identity characters of a user transmitted to a server location from a terminal unit;

transmitting the key information from the server location to said terminal unit;

applying said key information to a key generating algorithm to generate a user key;

generating a temporary validation key in response to a user request signal requesting downloading of digital information;

encrypting said temporary validation key by utilizing said user key and a key encryption algorithm to thereby generate user authorization information;

generating a header in response to said user authorization information, said header including said user authorization information;

encrypting the digital information requested by the user of said terminal unit to generate encrypted digital content;

combining the header and the encrypted digital content to form a copyright protection protocol;

transmitting the copyright protection protocol from the server location to said terminal unit;

receiving and storing, at said terminal unit, said key information transmitted from said server location;

receiving and storing, at said terminal unit, said copyright protection protocol;

generating a second user key in response to the stored key information;

analyzing said user authorization information in response to said second user key to determine whether the user is authorized to receive said encrypted digital information, and when said user is authorized to receive said encrypted digital information,utilizing said second user key to decrypt said temporary validation key from said user authorization information; and

decrypting said encrypted digital content the decrypted temporary validation key being used to decrypt to restore said digital information.

11.
96. (previously presented) The method of claim 95, 10 further comprising a step of transmitting information relating to a service fee to a service sanction agent server, said information being generated when said encrypted digital content is transmitted to said terminal unit.

12.
97. (previously presented) The method of claim 95, 10 further comprising a step of applying said user key to a hash algorithm at said server location to generate a hash value, said hash value being added to said header.

13. 98. (previously presented) The method of claim 12 97, further comprising a steps of:

applying said second user key to a hash algorithm in said terminal unit to generate a second hash value; and

comparing said hash value in said header to said second hash value, and when the second hash value is determined to coincide with the hash value in the header, the user is recognized to be authorized and the temporary validation key is decrypted using the user key.

## REMARKS

The indication of allowable subject matter with respect to claims 32, 74, 81, 83, 84 and 95-98 is appreciated.

Claims 23-24 were rejected under 35 U.S.C. §112, second paragraph based upon a number of deficiencies kindly noted by the Examiner. The Applicant respectfully traverses this rejection for the following reason(s).

The Examiner objects to the term "the user" in line 17 of claim 23 as having insufficient antecedent basis, however, there is proper antecedents in line 5 which calls for "a user." Accordingly, the rejection is deemed to be in error, but is now moot in view of the cancellation of claims 23 and 24.

Claims 20-27, 29, 70-71, 73-80, 82 and 85-88 were rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Pinder et al. (*hereafter*: Pinder) in view of Weber.

The rejection is deemed moot in view of the foregoing amendment wherein claims 20-24, 27, 29-32, 34-72, 74-76, 78, 80-82 and 85-94 have been canceled. Claim 25 has been amended to include the features of claims 27, 31 and 32 of which claim 32 has been deemed allowable by the Examiner. Claim 28 has been amended to include the features of claims 25 (from which it depended), claim 31 and claim 32 of which claim 32 has been deemed allowable by the Examiner. Claim 73 has been amended to include the features of claims 70 (from which it depended) and claim

74 of which claim 74 has been deemed allowable by the Examiner. Claim 79 has been amended to include the features of claims 80 and 81 of which claim 81 has been deemed allowable by the Examiner. And claim 83 has been amended to include the features of claims 79 and 82 (from which it depended), claim 83 has been deemed allowable by the Examiner.

Accordingly, no new claims have been entered, no new issues are raised by the foregoing amendment, and all the pending claims are now in condition for allowance. Therefore, the foregoing amendment should be entered.

Additionally, in view of the Continuation Application being filed including the rejected claims, the Applicant respectfully traverses this rejection for the following reason(s).

Claim 20 calls for, in part, *a protocol format generator located at a server location, said protocol format generator generating a copyright protection protocol by utilizing key information generated in response to identity characters of a user transmitted to said server location from a terminal unit, said copyright protection protocol including a header and digital contents.*

Neither Pinder nor Weber describe a ***copyright protection protocol*** being generated at a server location. A word search of both references fail to find mention of the term ***copyright*** nor a definition supporting the Examiner's holding that Pinder provides the necessary teaching for *copyright protection protocol.*

The Examiner has referred us to Pinder's Fig. 6 and col. 4, lines 1-26 with respect to a *protocol format generator*; col. 12, lines 47-58 with respect to *identity characters of a user*; and Figs. 6 and 10 with respect to a *copyright protection protocol including a header and digital*

*contents.*

In Pinder, Fig. 6 is a block diagram of the conditional access system in the digital broadband delivery system of Fig. 5, and Fig. 10 is a diagram of how ECMs (entitlement control messages) are mapped into a MPEG-2 transport stream.

The entitlement control messages contain information needed to decrypt the encrypted portion of the associated instance data 109. A given entitlement control message is sent many times per second, so that it is immediately available to any new viewer or a service. In order to make decryption of instance data 109 even more difficult for pirates, the content of the entitlement control message is changed every few seconds, or more frequently. For example, the History Channel is a service that provides television programs about history. Each program provided by the History Channel is an "instance" of that service. When the service distribution organization broadcasts an instance of the service, it encrypts or scrambles the instance to form encrypted instance 105. Encrypted instance 105 contains instance data 109, which is the encrypted information making up the program, and entitlement.

The encryption and decryption techniques used for service instance encoding and decoding belong to two general classes: symmetrical key techniques and public key techniques. A symmetrical key encryption system is one in which each of the entities wishing to communicate has a copy of a key; the sending entity encrypts the message using its copy of the key and the receiving entity decrypts the message using its copy of a the key. An example symmetrical key encryption-decryption system is the Digital Encryption Standard (DES) system. A public key encryption system is one in which each of the entities wishing to communicate has its own public key-private key pair. A message encrypted with the public key can only be decrypted with the private key and vice-versa.

Thus, as long as a given entity keeps its private key secret, it can provide its public key to any other entity that wishes to communicate with it. The other entity simply encrypts the message it wishes to send to the given entity with the given entity's public key and the given entity uses its private key to decrypt the message. Where entities are exchanging messages using public key encryption, each entity must have the other's public key. The private key can also be used in digital signature operations, to provide authentication.

Regarding the above cited feature of claim 20, Pinder fails to teach *identity characters of a user transmitted to said server location from a terminal unit*, and more particularly fails to teach *generating a copyright protection protocol by utilizing key information generated in response to identity characters of a user transmitted to said server location from a terminal unit.*

The Examiner states that Pinder "do not disclose that the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data."

As noted above, the Pinder invention uses symmetrical key techniques and public key (public key-private key pair) techniques. There does not appear to be a need for a server where the server responds to a user after receiving the user's ID by providing keys for decryption of the content encrypted data, in Pinder.

Here, the Examiner applies Weber's apparent teaching of communication from a user to a server where the server responds to the user after receiving the user's ID by providing keys for decryption of the content encrypted data. The Examiner has referred us to Weber's Abstract, and Figs. 2, 3, 4, 6a, 6b, 8, 9, 10, 12a, 12b and 14, which the Applicant has reviewed but find no mention

of a user's ID being used to generate a copyright protection protocol. Weber's specification is quite complicated, but has not been referred to by the Examiner to support the Examiner's suggetion of what Weber teaches. The Examiner is referred to 37 CFR §1.104(c)(2) which directs the Examiner to designate the particular part relied on as **nearly** as practicable, when a reference is complex or shows or describes inventions other than that claimed by the applicant. Clearly Pinder and Weber show or describe inventions other than that claimed by the applicant, or a §103(a) rejection would not have been made. The pertinence of each reference, if not apparent, must be clearly explained.

Note, *Ex parte Levy*, 17 USPQ2d 1461, 1462 (1990) states:

> "it is incumbent upon the examiner to identify wherein each and every facet of the claimed invention is disclosed in the applied reference."

We note here that Weber illustrates in Fig. 2 a client certificate 240 which Weber describes as enabling a merchant computer system 130 to authenticate the identity of a **customer computer system 120**. Also illustrated in Fig. 2 is a server key exchange message 225. Server key exchange message 225 identifies a key that may be used by a customer computer system 120 to decrypt further messages sent by merchant computer system 130 (server). From the foregoing, it must be shown that Weber's server key exchange message 225 is generated using a user's ID, in order to establish a *prima facie* basis of obviousness.

*In re Rijckaert*, 28 USPQ2d 1955 (CAFC 1993) states:

> "A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 782, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rhinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976). If the examiner fails to establish a *prima facie* case, the

rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

A further review of Weber's specification finds no teaching that server key exchange message 225 is generated using a user's ID nor any other ID such as client certificate 240 nor the identity of customer computer system 120.

As for Weber's Figs. 2, 3, 4, 6a, 6b, 8, 9, 10, 12a, 12b and 14, these figures concern a method of securely supplying payment information to a payment gateway in order to obtain payment authorization. There does not appear to be any teaching, with respect to these figures, concerning *generating a copyright protection protocol.*

Accordingly, we find no *prima facie* showing that Weber teaches what the Examiner suggests Weber teaches.

Accordingly, the rejection of claim 20 is deemed to be in error and should be withdrawn.

Applicant has reviewed Pinder and Weber further, and finds no mention of *identity characters of a user*, nor any equivalency thereto. According to the present invention *identity characters of a user* may be, for example, a social security number or a drivers licence number. The advantage of utilizing *identity characters of a user* is that the user is not limited to a particular playback apparatus or personal computer for receiving downloaded digital information.

In Paper No. 21, paragraph 9, the Examiner provides an untenable argument regarding a plate number of a car, for example, not only identify the car but also the car's owner, as identifying a user.

The Examiner should consider that although a plate number of a car may identify a car the

car's owner, it does not identify who used the car. For example, if a witness gets a car's plate number, said car having been involved in a felony hit and run, and the car turned out to be owned by the Examiner, will the Examiner admit to the hit and run if he loaned the car to a friend and it was the friend that was the car's user and involved in the hit and run. We don't think so, and believe the Examiner would the identify the car's user to the authorities.

Claim 20 also calls for, in part, *a protocol format decoder located at said terminal unit, said protocol format decoder having a decryption algorithm, said protocol format decoder storing the key information generated by the protocol format generator, said protocol format decoder decrypting and replaying the digital contents according to the stored key information and the information of the header received from the protocol format generator.*

Pinder and Weber fail to teach the foregoing feature of the present invention, and the Examiner fails to provide any hint as to where the feature is found in the applied art, thus failing to establish a *prima facie* basis of obviousness.

Accordingly, the rejection of claim 20 is deemed to be in error and should be withdrawn.

Additionally, claim 23 calls for, in part, *said protocol format generator applying said key information to a key generating algorithm to generate a user key utilized to generate a temporary validation key, said temporary validation key being encrypted to generate user authorization information, said header including said user authorization information.*

The Examiner fails to identify where the whole of the foregoing feature is taught by the

applied art. The Examiner indicates that Pinder teaches a *temporary validation*, but also indicates that such *temporary validation* is generated randomly, instead of being generated in response to a user key generated by a key generation algorithm in response to key information corresponding to identity characters of a user.

Accordingly, the rejection of claim 23 is deemed to be in error and should be withdrawn.

Claims 21-27, 29, 70-71, 73-80, 82 and 85-88 are deemed to be allowable over the applied art at least for the reasons discussed above with respect to claim. For example, similar to claim 20, claim 23 calls for *generating a copyright protection protocol by generating key information using random numbers, said key information corresponding to identity characters of a user transmitted to said server location from a terminal unit*; claim 25 calls for *key data being randomly generated in response to identity characters of a user transmitted to a host server from a terminal unit*; claim 70 calls for *producing said key information in response to said identity characters transmitted from said terminal unit*; and claim 79 calls for *host server responding to said identity characters* (of a user: lines 3-4) *transmitted from said service server for producing said key information.*

Accordingly, since neither reference teaches using identity characters of a user to generate key information at a sever, then the rejection of claims 21-27, 29, 70-71, 73-80, 82 and 85-88 is deemed to be in error and should be withdrawn.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Should a Petition for extension of time be required with the filing of this Response, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if,** a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P55501
Date: 6/2/04
I.D.: REB/MDP